Discrete Mathematics 18 (1977) 79–85.

SKEW-HADAMARD MATRICES OF ORDER $2(q+1)$

Edward SPENCE
University of Glasgow, Glasgow G12 8QW, Scotland

Received 29 May 1975
Revised 18 May 1976

Szekeres has established the existence of a skew-Hadamard matrix of order $2(q+1)$ in the case $q \equiv 5 \pmod 8$, a prime power. His method utilized complementary difference sets in the elementary abelian group of order q. The main result of this paper is to show that, for the same q, there exist skew-Hadamard matrices of order $2(q+1)$ that are of the Goethals–Seidel type. This is achieved by using a cyclic relative difference set with parameters $(q+1, 4, q, \frac{1}{4}(q-1))$.

1. Introduction

A Hadamard matrix H is a square matrix of order n with entries ± 1 and which satisfies $HH^T = nI$, where H^T denotes the transpose of H and I is the $n \times n$ identity matrix. It is easy to see that for H to exist n must be 1, 2 or a multiple of 4. The smallest order for which the existence of a Hadamard matrix is still in doubt is 268.

A Hadamard matrix H is said to be skew-Hadamard if $H - I$ is skew-symmetric. Many families of skew-Hadamard matrices are known. A comprehensive list of references may be found in [9]. One result which is relevant to the topic of this paper is due to Szekeres [6] who proved that if q is a prime power $\equiv 5 \pmod 8$ then there exists a skew-Hadamard matrix of order $2(q+1)$. Skew-Hadamard matrices of the same orders are constructed in this paper, but the method used and the type of skew-Hadamard matrix obtained are completely different to that found by Szekeres. The method uses a construction due to Goethals and Seidel [3] who proved the following theorem.

Theorem 1.1. *Let R be the square matrix of order n whose only non-zero entries satisfy $r_{i,n-2-i} = r_{n-1,n-1} = 1$ $(0 \leq i \leq n-2)$. Then if A, B, C, D are circulant ± 1 matrices of order n satisfying*

$$AA^T + BB^T + CC^T + DD^T = 4nI,$$

the matrix

$$H = \begin{bmatrix} A & BR & CR & DR \\ -BR & A & -D^TR & C^TR \\ -CR & D^TR & A & -B^TR \\ -DR & -C^TR & B^TR & A \end{bmatrix} \tag{1.1}$$

is a Hadamard matrix of order $4n$. *Further, if* $A - I$ *is skew-symmetric then* H *is skew-Hadamard.*

Whiteman [11] used the above construction to obtain skew-Hadamard matrices of the Goethal–Seidel type of order $q + 1$ where q is a prime power $\equiv 3 \pmod 8$. It is perhaps worthwhile pointing out that Whiteman's result (but not his proof) is contained implicitly in a paper of Delsarte, Goethals and Seidel ([1] Theorem 4.3 (ii)).

The main result of this paper is the following.

Theorem 1.2. *If* $q \equiv 5 \pmod 8$ *is a prime power then there exists a skew-Hadamard matrix of order* $2(q + 1)$ *of the Goethals–Seidel type.*

The proof of Theorem 1.2 uses relative difference sets which are described in the next section. (For further applications of relative difference sets to the construction of Hadamard matrices, the reader is referred to [4] and [5].)

In his paper [6] Szekeres conjectured that there exists a skew-Hadamard matrix of order $2(q + 1)$ when q is a prime power $\equiv 1 \pmod 8$. It may be that the method of this paper can be adapted to prove this result, but the author has so far been unsuccessful in his attempts.

2. Relative difference sets

Definition 2.1. A set $D = \{d_1, d_2, \ldots, d_k\}$ of k elements in an additive abelian group G of order rs is said to be a difference set in G relative to a subgroup H of order s if the elements of D are distinct coset representatives of H in G and if for each $g \in G - H$ there exist exactly λ pairs (d_i, d_j) with $d_i, d_j \in D$ such that $d_i - d_j = g$. Such a relative difference set will be denoted by $D(r, s, k, \lambda)$. For further details of relative difference sets see [2] which will be referred to for proofs of results used.

The rational integer t is said to be a multiplier of the relative difference set $D(r, s, k, \lambda)$ if $\{td : d \in D\} = \{d + g : d \in D\}$ for some $g \in G$. If $g = 0$, D is said to be fixed by t. For any $x \in G$, $D + x = \{d + x : d \in D\}$ is called a translate of D. Observe that a translate of D is also a relative difference set in G with the same parameters as D.

In this paper we consider cyclic relative difference sets (i.e. relative difference sets in a cyclic group) with parameters $(q + 1, 4, q, \frac{1}{4}(q - 1))$ where $q \equiv 5 \pmod 8$ is a

prime power. The existence of these relative difference sets is guaranteed by Corollary 5.1.1 of [2]. Also applying Theorem 7.1 of [2] immediately yields that q is a multiplier of a $D(q+1, 4, \frac{1}{4}(q-1))$ relative difference set in the cyclic group of order $4(q+1)$, and by Theorem 8.2 of [2] we may assume D fixed by q (for there is a translate of D fixed by q).

We require the following lemma.

Lemma 2.2. *Let D be a $(q+1, 4, q, \frac{1}{4}(q-1))$ cyclic relative difference set fixed by q where $q \equiv 5 \pmod 8$. Then one and only one of $0, q+1, 2(q+1), 3(q+1)$ belongs to D.*

Proof. Since D is fixed by q the elements of D can be paired (d, qd) except when $d \equiv qd \pmod{4(q+1)}$, i.e. unless $d(q-1) \equiv 0 \pmod{4(q+1)}$ which is equivalent to $d \equiv 0 \pmod{(q+1)}$. Since the number of elements in D, namely q, is odd, it follows that precisely one such multiple of $q+1$ belongs to D (for the elements of D are incongruent $\bmod(q+1)$). This completes the proof.

Following this lemma we may assume that $0 \in D$, for $D + l(q+1)$ is also fixed by q for any integer l. Also, it is a simple matter to see that the number of even integers in D is $\frac{1}{2}(q+1)$ while the number of odd integers in D is $\frac{1}{2}(q-1)$.

Consider now the set $D \cup D + q + 1$; it has $2q$ distinct elements $(\bmod 4(q+1))$. For each i let a_i denote the unique integer $(\bmod 8)$ such that

$$a_i(q+1)/2 + i \equiv 0 \pmod 8, \tag{2.1}$$

and for each i let

$$D_i = \left\{ \frac{d + a_i(q+1)/2}{8} \left(\bmod \frac{q+1}{2} \right) : d \in D \cup D + q + 1,\ d \equiv i \pmod 8 \right\}.$$

We then have

Lemma 2.3.

(i) $D_i = -D_{5i}$,
(ii) $x \in D_i \iff -x \notin D_i$,
} *if i is odd,*

(iii) $x \in D_i \iff -x \in D_i$,
(iv) $D_i \cup D_{i+4} = \{0, 1, 2, \ldots, (q-1)/2\}$
} *if i is even.*

Proof. (i) Suppose first that i is odd and that $x \in D_i$. Then there exists $d \in D \cup D + q + 1$ such that $d \equiv i \pmod 8$ and $d + a_i(q+1)/2 \equiv 8x \pmod{4(q+1)}$. Since $D \cup D + q + 1$ is fixed by q it follows that $qd \in D \cup D + q + 1$. Moreover $qd \equiv 5i \pmod 8$. Thus there exists $y \in D_{5i}$ such that $qd + a_{5i}(q+1)/2 \equiv 8y \pmod{4(q+1)}$. But $a_{5i} \equiv 5a_i \pmod 8$, so that

$$\begin{aligned} 8y &\equiv qd + 5a_i(q+1)/2 \pmod{4(q+1)} \\ &\equiv -8x + (q+1)(d + 3a_i) \pmod{4(q+1)}. \end{aligned}$$

However, from (2.1) it is seen that $i + 3a_i \equiv 0 \pmod 4$ since $q \equiv 5 \pmod 8$. Thus we deduce that $y \equiv -x \pmod{(q+1)/2}$ which proves that $-D_i \subseteq D_{5i}$. Replacing i by $5i$ proves (i).

(ii) Suppose x and $-x$ both belong to D_i. Then there exist $d_1, d_2 \in D \cup D + q + 1$ such that $d_1 \equiv d_2 \equiv i \pmod 8$ and

$$[d_1 + a_i(q+1)/2] + [d_2 + a_i(q+1)/2] \equiv 0 \pmod{4(q+1)},$$

which is equivalent to

$$d_1 + d_2 + a_i(q+1) \equiv 0 \pmod{4(q+1)}. \tag{2.2}$$

However, d_1, qd_1 both belong to $D \cup D + q + 1$ and

$$d_1 + qd_1 \equiv (q+1)d_1 \equiv i(q+1) \pmod{4(q+1)}. \tag{2.3}$$

Thus from (2.2) and (2.3) we obtain

$$\begin{aligned} qd_1 - d_2 &\equiv (i + a_i)(q+1) \pmod{4(q+1)} \\ &\equiv 2(q+1) \pmod{4(q+1)}. \end{aligned}$$

But this is impossible since the elements of $D \cup D + q + 1$ are incongruent $\pmod{2(q+1)}$. Hence $x \in D_i \Rightarrow -x \notin D_i$. To prove the converse, observe that $x \in D_i \Rightarrow -x \notin D_i$ gives $|D_i| \leq (q-1)/4$. However, since $D \cup D + q + 1$ contains $q - 1$ odd integers we have

$$|D_1| + |D_3| + |D_5| + |D_7| = q - 1,$$

which shows that $|D_i| = (q-1)/4$ (i odd). This, together with $x \in D_i \Rightarrow -x \notin D_i$, establishes (ii).

To prove (iii), (iv), suppose now that i is even. Let $x \in D_i$ so that $d + a_i(q+1)/2 \equiv 8x \pmod{4(q+1)}$ for some $d \in D \cup D + q + 1$, $d \equiv i \pmod 8$. Then $qd \in D \cup D + q + 1$ and $qd \equiv 5i \equiv i \pmod 8$, since i is even. Thus there exists $y \in D_i$ such that $qd + a_i(q+1)/2 \equiv 8y \pmod{4(q+1)}$. However, $8(x+y) \equiv (q+1)(d + a_i) \equiv 0 \pmod{4(q+1)}$. Thus $y \equiv -x \pmod{(q+1)/2}$ and (iii) is proved. Finally, to prove (iv) we show that

$$D_i \cap D_{i+4} = \emptyset \qquad (i \text{ even}). \tag{2.4}$$

For suppose not. Then there exist $d_1, d_2 \in D \cup D + q + 1$ such that $d_1 \equiv i \pmod 8$, $d_2 \equiv i + 4 \pmod 8$ and

$$d_1 + a_i(q+1)/2 \equiv d_2 + a_{i+4}(q+1)/2 \pmod{4(q+1)}.$$

Then

$$\begin{aligned} d_1 - d_2 &\equiv (a_{i+4} - a_i)(q+1)/2 \pmod{4(q+1)} \\ &\equiv 2(q+1) \pmod{4(q+1)}, \end{aligned}$$

which, as has been pointed out before, is [illegible].

If D has n_0 integers congruent to 0 (mod [illegible] n_2 integers congruent to 2 (mod 4)

then $n_0 + n_2 = \frac{1}{2}(q+1)$. Also, it follows that $D + q + 1$ has n_2 integers congruent to $0 \pmod 4$ and n_0 integers congruent to $2 \pmod 4$. Hence $|D_i| + |D_{i+4}| = n_0 + n_2 = \frac{1}{2}(q+1)$ (if i is even). This together with (2.4) completes the proof of the lemma.

We are now in a position to prove:

Theorem 2.4. *If there exists a cyclic relative difference set D with parameters $(q+1, 4, q, \frac{1}{4}(q-1))$ where $q \equiv 5 \pmod 8$ then there exists a skew-Hadamard matrix of order $2(q+1)$ of the Goethals–Seidel type.*

Proof. Let $q + 1 = 2m$ so that $m \equiv 3 \pmod 4$ and let $\phi(x) \equiv \sum_{d \in D} x^d \pmod{x^{8m} - 1}$ be the Hall polynomial for D. Then

$$\phi(x)\phi(x^{-1}) \equiv 2m - 1 + \tfrac{1}{2}(m-1)(T_{8m}(x) - T_4(x^{2m})) \pmod{x^{8m} - 1}, \tag{2.5}$$

where $T_r(x) = 1 + x + x^2 + \cdots + x^{r-1}$. Hence

$$\begin{aligned}(1 + x^{2m})(1 + x^{6m})\phi(x)\phi(x^{-1}) \equiv{}& 2(2m-1) + 2(m-1)(T_{8m}(x) - T_4(x^{2m})) \\ &+ (2m-1)(x^{2m} + x^{6m}) \pmod{x^{8m} - 1}.\end{aligned} \tag{2.6}$$

Note that $(1 + x^{2m})\phi(x)$ is the incidence polynomial for the set $D \cup D + q + 1 = B$, say. Let $B_i = \{b \in B : b \equiv i \pmod 8\}$ and write $\phi_i(x) \equiv \sum_{b \in B_i} x^b \pmod{x^{8m} - 1}$. Then, picking out the eighth powers of x from (2.6) yields

$$\sum_{i=0}^{7} \phi_i(x)\phi_i(x^{-1}) \equiv 2m + 2(m-1)T_m(x^8) \pmod{x^{8m} - 1}. \tag{2.7}$$

Now let $\psi_i(x^8) \equiv \phi_i(x)x^{a_i m} \pmod{x^{8m} - 1}$, so that (2.7) becomes

$$\sum_{i=0}^{7} \psi_i(x)\psi_i(x^{-1}) \equiv 2m + 2(m-1)T_m(x) \pmod{x^m - 1}. \tag{2.8}$$

It is a simple matter to see that $\psi_i(x) \equiv \sum_{d \in D_i} x^d \pmod{x^m - 1}$ where D_i is as in Lemma 2.3 (with $m = (q+1)/2$). Then Lemma 2.3 can be expressed in terms of the $\psi_i(x)$ as follows

$$\left.\begin{aligned}&\text{(i) } \psi_i(x) \equiv \psi_{8i}(x^{-1}) \pmod{x^m - 1},\\ &\text{(ii) } \psi_i(x) + \psi_i(x^{-1}) \equiv T_m(x) - 1 \pmod{x^m - 1},\end{aligned}\right\} \text{ if } i \text{ is odd,}$$

$$\left.\begin{aligned}&\text{(iii) } \psi_i(x) \equiv \psi_i(x^{-1}) \pmod{x^m - 1},\\ &\text{(iv) } \psi_i(x) + \psi_{i+4}(x) \equiv T_m(x) \pmod{x^m - 1},\end{aligned}\right\} \text{ if } i \text{ is even.} \tag{2.9}$$

Using these formulae in (2.8) we obtain, after simplification,

$$\sum_{i=0}^{3} \psi_i(x)\psi_i(x^{-1}) \equiv m - T_m(x)(1 - \psi_5(x) - \psi_2(x)) \pmod{x^m - 1}.$$

Thus

$$\begin{aligned}&\sum_{i=0}^{3} (2\psi_i(x) - T_m(x))(2\psi_i(x^{-1}) - T_m(x)) \equiv \\ &\quad \equiv 4m + 4T_m(x)(m - 1 - \psi_1(x) - \psi_3(x)) \pmod{x^m - 1}.\end{aligned}$$

However, if i is odd $T_m(x)\psi_i(x) \equiv \frac{1}{2}(m-1)\,T_m(x) \pmod{x^m-1}$, so we finally obtain

$$\sum_{i=0}^{3} (2\psi_i(x) - T_m(x))(2\psi_i(x^{-1}) - T_m(x)) \equiv 4m \pmod{x^m-1}.$$

Thus if $2\psi_i(x) - T_m(x) \equiv b_{i0} + b_{i1}x + \cdots + b_{i,m-1}x^{m-1} \pmod{x^m-1}$, the circulant $m \times m$ matrices B_0, B_1, B_2, B_3 whose first rows are $(b_{i0}, b_{i1}, \ldots, b_{i,m-1})$ $(0 \leq i \leq 3)$ are ± 1 matrices which satisfy $\sum_{i=0}^{3} B_i B_i^T = 4mI$.

Condition (2.9) ensures that B_0 and B_2 are symmetric, while $B_1 + I$ and $B_3 + I$ are both skew-symmetric.

Hence if we take $A = -B_1$, $B = B_0$, $C = B_2$, $D = B_3$ in (1.1), the resulting matrix H of order $4m = 2(q+1)$ is skew-Hadamard of the Goethals–Seidel type. This proves the theorem.

As was mentioned earlier, cyclic relative difference sets with parameters $(q+1, 4, q, \frac{1}{4}(q-1))$ exist if $q \equiv 5 \pmod 8$ is a prime power. Thus we have constructed a (new) infinite family of skew-Hadamard matrices of the Goethals–Seidel type. Also, in her paper [8], Wallis defines G-matrices and uses them extensively in constructing Baumert–Hall arrays. The matrices $B_0, B_2, B_1 + I$ and $B_3 + I$ above are G-matrices, being members of the first infinite class of such matrices to be found.

Example 2.5. It is easy to verify that the set $D = \{0, 1, 3, 4, 6, 12, 13, 22, 33, 37, 39, 44, 52\}$ is a cyclic relative difference set with parameters $(14, 4, 13, 3)$ in the cyclic group of integers modulo 56. The sets D_0, D_1, D_2, D_3 of Lemma 2.3 are $\pmod 7$ $D_0 = \{0\}$, $D_1 = \{1, 3, 5\}$, $D_2 = \{2, 3, 4, 5\}$, $D_3 = \{2, 3, 6\}$ giving circulant matrices B_0, B_1, B_2, B_3 with first rows $(+ - - - - - - -)$, $(- + - + - + -)$, $(- - + + + + -)$, $(- - + + - - +)$ respectively ($+$ denotes $+1$, $-$ denotes -1). This yields a skew-Hadamard matrix of order $2(13+1) = 28$ of the Goethals–Seidel type.

3. Final remarks

Using similar arguments the following two results (implicit in [1]) can be proved:

Theorem 3.1. (Turyn [7], Whiteman [10]). *If there exists a cyclic relative difference set with parameters $(2v, 2, 2v-1, v-1)$ where v is odd (in particular if $2v - 1 \equiv 1 \pmod 4$ is a prime power) then there exists a Hadamard matrix of order $4v$ of the Williamson type.*

Theorem 3.2. (Whiteman [11]). *If there exists a cyclic relative difference set with parameters $(4u, 2, 4u-1, 2u-1)$ where u is odd (in particular, if $4u - 1 \equiv 3 \pmod 8$*

is a prime power) then there exists a skew-Hadamard matrix of order $4u$ *of the Goethals–Seidel type.*

References

[1] P. Delsarte, J.M. Goethals and J.J. Seidel, Orthogonal matrices with zero diagonal, II. Can. J. Math. 23 (1971) 816–832.
[2] J.E.H. Elliott and A.T. Butson, Relative difference sets, Illinois J. Math. 10 (1966) 517–531.
[3] J.M. Goethals and J.J. Seidel, A skew-Hadamard matrix of order 36, J. Austr. Math. Soc. 11 (1970) 343–344.
[4] E. Spence, Skew-Hadamard matrices of the Goethals–Seidel type, Can. J. Math. 27 (1975) 555–560.
[5] E. Spence, Hadamard matrices from relative difference sets, J. Comb. Theory Ser. A 19 (1975) 287–300.
[6] G. Szekeres, Tournaments and Hadamard matrices, Enseignment Math. 15 (1969) 269–278.
[7] R.J. Turyn, An infinite class of Williamson matrices, J. Comb. Theory Ser. A 12 (1972) 319–321.
[8] J.S. Wallis, On Hadamard matrices, J. Comb. Theory Ser. A 18 (1975) 149–164.
[9] W.D. Wallis, A.P. Street and J.S. Wallis, Room squares, sum-free sets, Hadamard matrices, Lecture Notes in Mathematics, no. 292 (Springer-Verlag, Heidelberg, 1972).
[10] A.L. Whiteman, An infinite family of Hadamard matrices of the Williamson type, J. Comb. Theory Ser. A 14 (1973) 334–340.
[11] A.L. Whiteman, Skew-Hadamard matrices of Goethals–Seidel type, Discrete Math. 2 (1972) 397–405.